(6)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-308264
(43)Date of publication of application : 05.11.1999

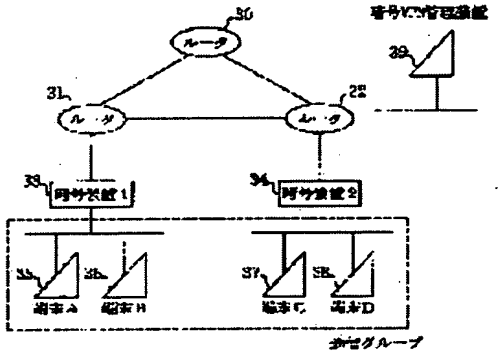
(51)Int.CI. H04L 12/46
H04L 12/28
G06F 13/00
H04L 9/08
H04L 9/14
H04L 9/36
H04L 12/66
H04L 12/56

(21)Application number : 10-107808
(22)Date of filing : 17.04.1998

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : NAGASHIMA NORIMITSU
INADA TORU
IDEGUCHI TETSUO
WATANABE AKIRA

(54) CRYPTOCOMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce a load on a network manager at the time of setting a cipher device and to eliminate an overhead at the time of starting cryptographic communication by specifying a communication group using a block diagram of the network, obtaining a communication path of a communication terminal, preparing a cryptographic communication control table and distributing it to the cipher device.
SOLUTION: A cipher VPN management device 39 selects a cipher device which communicates by using a network block diagram, specifies a communication group, obtains communication path for communication terminals 35 to 38 of the specified communication group, prepares a cryptographic communication control table to be distributed to cipher device 33 and 34. Thus, the communication paths are clarified in the communication between the communication terminals 35 and 38 and operation mistakes by manually setting cryptographic communication information are made fewer. Also, when communication data from the terminals 35 to 38 are received, it is possible to eliminate an overhead at the time of starting the cryptographic communication since the cipher device 33 and 34 hold the cryptographic communication control table and there is no need to transmit a key search packet.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－308264

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]		識別記号	FI	
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ　11/00	３１０Ｃ
	12/28		Ｇ０６Ｆ　13/00	３５１Ｚ
Ｇ０６Ｆ	13/00	３５１	Ｈ０４Ｌ　9/00	６０１Ｚ
Ｈ０４Ｌ	9/08			６４１
	9/14			６８５

審査請求　未請求　請求項の数４　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平10－107808

(22)出願日　平成10年(1998)４月17日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　永島　規充
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　稲田　徹
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

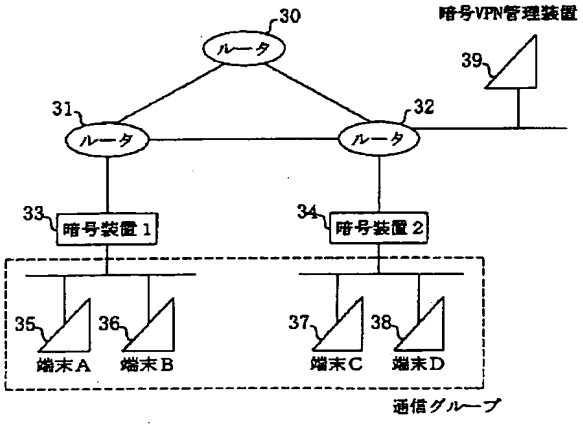
(72)発明者　井手口　哲夫
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　弁理士　宮田　金雄　（外２名）

最終頁に続く

(54)【発明の名称】　暗号通信システム

(57)【要約】
【課題】　大規模ネットワークにおいても暗号通信のためのネットワーク管理を容易にし、かつ暗号通信時のオーバヘッドをなくし、暗号通信経路を明確化する。
【解決手段】　ネットワーク構成図を暗号ＶＰＮ管理装置に表示、構成図上で暗号通信グループを指定し、通信グループ内のすべての端末の通信経路を検索し、通信経路上にある暗号装置の暗号通信制御テーブルを作成し、暗号装置に配送する。



1

【特許請求の範囲】

【請求項１】　通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてＶＰＮ（Virtual　Private　Network）を管理する暗号ＶＰＮ管理装置とを有する暗号通信システムにおいて、

前記暗号ＶＰＮ管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、

通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、

この指定された通信グループに属する通信端末間の暗号通信において使用する鍵ＩＤを設定する鍵ＩＤ設定手段と、

前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コード及び暗号鍵ＩＤを含む暗号通信制御テーブルを通信経路上の前記暗号装置毎に作成する暗号通信制御テーブル作成手段と、

これを各暗号装置に配送する配送手段を有し、

前記暗号装置は、受け取った前記暗号通信制御テーブルに基いて通信データを処理する通信データ処理手段を有することを特徴とする暗号通信システム。

【請求項２】　通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてＶＰＮ（Virtual　Private　Network）を管理する暗号ＶＰＮ管理装置とを有する暗号通信システムにおいて、

前記暗号ＶＰＮ管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、

前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コードを含む暗号通信制御テーブルを通信経路上の暗号装置毎に作成する暗号通信制御テーブル作成手段と、制御コードが暗号の場合には暗号鍵を生成して前記暗号通信制御テーブルに設定する暗号鍵設定手段と、

2

これを各暗号装置に配送する配送手段とを有し、

前記暗号装置は、受け取った前記暗号通信テーブル及び暗号鍵に基いて通信データを処理する通信データ処理手段を有することを特徴とする暗号通信システム。

【請求項３】　前記通信グループ指定手段により指定された通信グループに属する通信端末間のすべての通信経路を検索して、各通信路においてデータ暗号化、復号を行う暗号装置が決定できない場合、指定した通信グループ内の通信が平文で行われることを示す確認メッセージを表示する確認メッセージ表示手段と確認結果に応じて暗号装置の処理を決定する処理決定手段を有することを特徴とする請求項１または請求項２に記載の暗号通信システム。

【請求項４】　前記暗号ＶＰＮ管理装置の暗号通信制御テーブル作成手段は、通信グループに対するセキュリティレベルを設定し、指定された通信グループが他の通信グループと重複する場合、前記設定されたセキュリティレベルに基づいて暗号通信制御テーブルを作成することを特徴とする請求項１または請求項２に記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータネットワークにおけるデータの機密を保持する暗号通信システムに関する。

【０００２】

【従来の技術】近年のコンピュータネットワークの普及に伴い、ネットワーク上のデータの機密を保持する通信データ暗号技術への関心が高まっている。従来、通信データの暗号については特開平６－２０９３１３に見られるように、暗号装置内部に保持している通信データの宛先、送信元アドレスの一方あるいはその両方に対応した暗号鍵を登録した暗号テーブルに従ってデータを暗号化、復号する方法がとられていた。しかし、暗号テーブルは、各暗号装置毎に異なるためネットワーク管理者はネットワークの構成及び通信端末のアドレスを考慮して各暗号装置に対応する暗号テーブルを作成する必要があり、特に、ネットワークが大規模になると通信端末数も増大し、暗号テーブルが非常に複雑になるという課題があった。

【０００３】この課題を解決するため、特願平９－１４３７５５　暗号通信システムのように、図１５のようなネットワーク構成において暗号鍵探索バケット（図１７）を用いて、通信端末間の通信経路上の暗号装置の暗号鍵情報を収集し、収集した暗号鍵情報に基づいて暗号鍵情報を自動的に図１６のような暗号鍵テーブルに学習し、通信端末間の通信データを各暗号装置が暗号化、復号、平文中継する方法がとられた。

【０００４】

【発明が解決しようとする課題】上述の方法では、通信

端末間で最初にデータ通信を始める場合、暗号鍵テーブル作成のため図１７に示される暗号鍵探索パケットが送信され、この暗号鍵探索パケットに対する応答を受け取ってからでないと、暗号通信が行えないため通信開始までのオーバヘッドが大きくなる問題があった。また、上述の方法では暗号装置が暗号鍵探索パケットを用いて、自動的に暗号鍵情報を収集、登録してしまうため、ネットワーク管理者が実際の通信の途中経路を把握することができない。さらに、インターネットを介してＬＡＮを接続するようなケースでは、暗号鍵探索パケットが暗号化されずにインターネット上を流れることになり、ファイアウォールなどで守られた企業ネットワークに、インターネットからの鍵探索パケットを通過させるのは安全性の問題があった。

【０００５】本発明は、このような暗号通信開始時のオーバヘッド、暗号通信経路の明確化及び企業ネットワークへの安全性に対応するためになされたもので、ネットワーク構成図を用いて、暗号通信のエリア、通信端末群が指定でき、暗号装置の接続箇所、通信端末間の通信における通信経路を明示して、暗号装置の設定時のネットワーク管理者の負荷を軽減すると共に暗号通信開始時のオーバヘッドをなくし、また企業ネットワークの安全性を損なうことなく暗号通信を実現することを目的としている。

【０００６】

【課題を解決するための手段】第１の発明に係る暗号通信システムは、通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてＶＰＮ（Virtual Private Network）を管理する暗号ＶＰＮ管理装置とを有する暗号通信システムにおいて、前記暗号ＶＰＮ管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、この指定された通信グループに属する通信端末間の暗号通信において使用する鍵ＩＤを設定する鍵ＩＤ設定手段と、前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コード及び暗号鍵ＩＤを含む暗号通信制御テーブルを通信経路上の前記暗号装置毎に作成する暗号通信制御テーブル作成手段と、これを各暗号装置に配送する配送手段を有し、前記暗号装置は、受け取った前記暗号通信制御テーブルに基いて通信データを処理する通信データ処理手段を有するものである。

【０００７】第２の発明に係る暗号通信システムは、通信ネットワークに収容された複数の通信端末と、それら通信端末間でやり取りするデータを中継、暗号化する暗号装置と、それら暗号装置からのデータを中継するルータとを有する通信ネットワークを構成し、この通信ネットワークを仮想的な私設ネットワークとしてみなしてＶＰＮ（Virtual Private Network）を管理する暗号ＶＰＮ管理装置とを有する暗号通信システムにおいて、前記暗号ＶＰＮ管理装置は、ルータ、通信端末及び暗号装置等のネットワーク構成図を表示する構成図表示手段と、この構成図に基づいて、通信エリア、通信端末、通信端末群あるいは暗号装置を選択して通信グループを指定する通信グループ指定手段と、前記通信グループに属する通信端末間のすべての通信経路を検索し、検索結果に基づいて各通信経路に対する暗号装置の処理を決定し、通信経路の送信元、宛先アドレス、通信データを暗号化、透過あるいは廃棄するかを示す制御コードを含む暗号通信制御テーブルを通信経路上の暗号装置毎に作成する暗号通信制御テーブル作成手段と、制御コードが暗号の場合には暗号鍵を生成して前記暗号通信制御テーブルに設定する暗号鍵設定手段と、これを各暗号装置に配送する配送手段とを有し、前記暗号装置は、受け取った前記暗号通信テーブル及び暗号鍵に基いて通信データを処理するものである。

【０００８】第３の発明に係る暗号通信システムは、前記通信グループ指定手段により指定された通信グループに属する通信端末間のすべての通信経路を検索して、各通信路においてデータ暗号化、復号を行う暗号装置が決定できない場合、指定した通信グループ内の通信が平文で行われることを示す確認メッセージを表示する確認メッセージ表示手段と、確認結果に応じて暗号装置の処理を決定する処理決定手段を有するものである。

【０００９】第４の発明に係る暗号通信システムは、前記暗号ＶＰＮ管理装置の暗号通信制御テーブル作成手段は、通信グループに対するセキュリティレベルを設定し、指定された通信グループが他の通信グループと重複する場合、前記設定されたセキュリティレベルに基づいて暗号通信制御テーブルを作成するものである。

【００１０】

【発明の実施の形態】実施の形態１．図１は、実施の形態１におけるネットワーク構成の例で、ルータ３台（３０～３２）、暗号装置１、２（３３、３４）、通信端末Ａ、Ｂ、Ｃ、Ｄ（３５～３８）及び暗号ＶＰＮ管理装置（３９）が接続されている。図２はこの発明の暗号通信システムを構成する暗号ＶＰＮ管理装置であり、図２において、１は、暗号装置を管理する暗号ＶＰＮ管理装置、２は送受信処理部で、通信データの受信処理、送信処理を実施し、３はキーボード、マウスの入力を制御する入力制御部、４はルータ、暗号装置及び通信端末等のネットワーク機器の構成図を表示する構成表示部、５は

ネットワーク構成図上でネットワーク管理者によって指定された通信グループの情報から暗号通信制御テーブルを生成する暗号テーブル演算部、６は前記暗号通信制御テーブルを暗号化する暗号処理部、７は暗号処理部６で暗号化された暗号通信制御テーブルを暗号装置に配送する配送処理部である。

【００１１】図３は、この発明の暗号通信システムを構成する暗号装置である。図３において１０は暗号装置、１３は通信データを暗号化、復号する暗号化・復号部、１４は通信データを透過的に中継する透過中継部、１５は通信データを廃棄する廃棄部、１７は暗号ＶＰＮ管理装置で作成、送信された暗号通信制御テーブルを受理するテーブル管理部、１８は前記受理した暗号通信制御テーブルを復号する復号部、１６は通信データの処理方法を示す暗号通信制御テーブル、１１はパブリックポート、２０はローカルポートである。これらのポートは暗号装置が通信データを暗号化するのか復号するのかを識別するもので、暗号装置はパブリックポート１１から受信した通信データを復号し、ローカルポート２０に送信し、ローカルポート２０から受信した通信データを暗号化し、パブリックポート１１に送信する。１２、１９は送受信処理部で通信データの受信処理、送信処理を実施する。

【００１２】次に図６を用いて動作について説明する。まずネットワーク管理者が暗号ＶＰＮ管理装置の構成表示部４を起動し、図１のようなネットワーク構成図を表示する（ステップ１）。構成表示部４は、ネットワーク管理者による手入力もしくはＳＮＭＰ（Simple Network Management Protocol）を用いて収集した情報を元にネットワーク構成図を表示する。次に、ネットワーク管理者は、マウス、キーボードを使用して通信を行う暗号装置（この例では暗号装置１、２（３３、３４））を選択し、通信グループを指定する（ステップ２）。本実施例の場合、暗号装置の下流に接続されているネットワークを通信グループとする。暗号装置で使用する暗号鍵ＩＤ（この例では暗号鍵ＩＤ＝１）を入力する（ステップ３）。入力制御部３は、画面のどの暗号装置が選択されたかを構成表示部４に通知する。構成表示部４は、通知された情報を元にネットワーク管理者が指定した通信グループに属するすべての通信端末、暗号装置のアドレス情報、通信経路及び暗号鍵ＩＤをテーブル演算部５に通知する。テーブル演算部５では、通知された通信経路から１つを取り出し（例えば、通信端末Ａ（３５）－暗号装置１（３３）－ルータ（３１）－ルータ（３２）－暗号装置２（３４）－通信端末Ｃ（３７））、この通信経路にある暗号装置に対して（例：暗号装置１（３３））、まずこの暗号装置がネットワーク管理者がステップ２で選択した暗号装置かチェックする（ステップ６）。選択した暗号装置でない場合は、通信経路の両端のアドレスをこの暗号装置の暗号通信制御テーブルの宛先、送信元アドレスに設定し、制御コードに透過中継を設定する（ステップ７）。ネットワーク管理者が選択した暗号装置の場合は、通信経路上にネットワーク管理者が選択した別の暗号装置が存在するかチェックし（ステップ８）、存在すれば、暗号通信制御テーブルに通信経路の両端のアドレスを設定し、制御コードを暗号、暗号鍵ＩＤにステップ３で入力されたものを設定し（ステップ１０）、図４のような暗号通信制御テーブル１６を作成する。存在しない場合は、制御コードを廃棄とし、暗号通信制御テーブルに設定する（ステップ９）。これを１つの通信経路に存在する暗号装置分（前記通信経路の場合は、経路上に存在する暗号装置の数は２である）処理する（ステップ５）。このステップ５～１０の処理を通知されたすべての通信経路分（図１のネットワーク構成での通信経路は、

経路１：通信端末Ａ（３５）－暗号装置１（３３）－ルータ（３１）－ルータ（３２）－暗号装置２（３４）－通信端末Ｃ（３７）

経路２：通信端末Ｂ（３６）－暗号装置１（３３）－ルータ（３１）－ルータ（３２）－暗号装置２（３４）－通信端末Ｃ（３７）

経路３：通信端末Ａ（３５）－暗号装置１（３３）－ルータ（３１）－ルータ（３２）－暗号装置２（３４）－通信端末Ｄ（３８）

経路４：通信端末Ｂ（３６）－暗号装置１（３３）－ルータ（３１）－ルータ（３２）－暗号装置２（３４）－通信端末Ｄ（３８）

経路５：通信端末Ａ（３５）－通信端末Ｂ（３６）

経路６：通信端末Ｃ（３７）－通信端末Ｄ（３８）

の６経路である）行い（ステップ４）、各暗号装置に対する暗号通信制御テーブル１６（図４）を完成させ、暗号処理部６でこれを暗号化し（ステップ１１）、テーブル配送部７、送受信処理部２を経由し、図５のようなフォーマットて暗号ＶＰＮ管理装置３９から暗号装置１、２（３３、３４）へ、暗号通信制御テーブル１６（図４）を配送する（ステップ１２）。

【００１３】配送された暗号通信制御テーブル１６（図４）は、暗号装置のローカルポート２０またはパブリックポート１１で受信され、テーブル復号部１８でデータを復号後、テーブル管理部１７で処理され、暗号装置内部に保存される。以降、暗号装置では、通信データを受信する度に、暗号通信制御テーブル１６を参照し、通信データの宛先、送信元アドレスが暗号通信制御テーブル内と一致した場合、制御コードに従い、制御コードが暗号となっている時は保持している暗号鍵の中から暗号鍵ＩＤに対応する暗号鍵で通信データを暗号化、復号する。制御コードが透過中継となっている場合は、データをそのまま中継する。通信データの宛先、送信元アドレスが暗号通信制御テーブルと一致しない場合は、データを廃棄する。

【００１４】以上のように、暗号ＶＰＮ管理装置でネットワーク構成図を用いて、通信する暗号装置を選択し、通信グループを指定し、指定された通信グループの通信端末のすべての通信経路を求め、暗号通信制御テーブルを作成し、暗号装置に配送するようにしているので、通信端末間の通信における通信経路が明確化され、通信端末のアドレスを元に人手により暗号通信情報を設定するより操作ミスを少なくできる。通信端末からの通信データを受信した場合も、暗号装置は暗号通信制御テーブル１６を保持しているため、鍵探索パケットを送信する必要がないので暗号通信開始時のオーバヘッドをなくすことができ、また企業ネットワークの安全性を損なうことなく暗号通信を実現することができる。上記例では、ネットワーク管理者がネットワーク構成図上で通信する暗号装置を選択しているが、図１の点線部のようにマウスで通信端末、通信端末群あるいはエリアを囲み通信グループを指定しても同様の効果を得ることができる。

【００１５】実施の形態２．実施の形態１では、暗号ＶＰＮ管理装置から暗号鍵ＩＤを含む暗号通信制御テーブルを配送する場合の例を示したが、本実施の形態では、次に暗号鍵ＩＤの代わりに暗号鍵を配送する場合の実施の形態を示す。図７は、この実施の形態２における暗号ＶＰＮ管理装置であり、図２に暗号鍵を生成する暗号鍵生成部５２を追加したものである。暗号装置は図２、ネットワーク構成は図１と同様である。次に動作について図９を用いて説明する。ネットワーク管理者が通信グループを指定し、指定された情報を元に暗号通信制御テーブル16（図８）を作成するまでの手順（ステップ１、３～９）は前記実施の形態１と同様であるが、ステップ８で通信経路上にネットワーク管理者が指定した暗号装置が存在する場合に、暗号通信制御テーブルに通信経路の両端の通信端末のアドレス及び制御コードに暗号を設定し（ステップ１３）、暗号鍵生成部において暗号鍵を生成し（ステップ１４）、図８に示されるような暗号通信制御テーブルに設定し、暗号装置へ送信する（ステップ１１、１２）。

【００１６】暗号装置では送付された暗号鍵を含む暗号通信制御テーブルを暗号装置内部に保存し、以降、通信データを受信する度に、暗号通信制御テーブル16（図８）を参照し、通信データの宛先、送信元アドレスが暗号通信制御テーブル内と一致した場合、制御コードに従い、コードが暗号となっている場合は、暗号通信制御テーブルにある暗号鍵で通信データを暗号化、復号する。制御コードが透過中継及び廃棄となっている場合は、実施の形態１と同様である。

【００１７】以上のように、暗号ＶＰＮ管理装置から暗号鍵も合わせて配送するようにしているので、暗号鍵ＩＤの重複や数の制限を無くし、保持している暗号鍵のリストが異なっているため鍵ＩＤが合っているにもかかわらず通信できないといった通信の不通状態を防ぐことができる。また、実施の形態１の効果が得られることは言うまでもない。以上の実施の形態２では、ネットワーク管理者がネットワーク構成図上で暗号装置を選択しているが、通信端末あるいはエリアを選択し、通信グループを指定することでも同様の効果を得ることができる。

【００１８】実施の形態３．実施の形態１では、ネットワーク管理者が通信を行う暗号装置を選択するようにしたものであるが、本実施の形態は暗号装置が接続されていない通信端末と通信する場合の実施の形態を示す。図１０は、本実施の形態におけるネットワーク構成図である。次に動作を図１２を用いて説明する。通信端末Ｃ、Ｄ（３７、３８）側に暗号装置は接続されていないので、ネットワーク管理者は、構成図上で暗号装置１（３３）と通信端末Ｃ，Ｄ（３７、３８）を選択し、通信グループを指定する（ステップ１、２）。以降のステップ３～８は図９と同様である。ステップ８では、通信経路上にネットワーク管理者が指定した暗号装置が存在するかチェックするが、暗号装置が存在しないので、ネットワーク管理者に対し、この通信経路における通信が透過中継になることの確認メッセージを表示し（ステップ１５）。応答がYes場合は、制御コードを透過中継とし暗号通信制御テーブル16（図１１）を設定する（ステップ７）。Noの場合は、制御コードを廃棄として暗号通信制御テーブルを設定し、（ステップ９）、暗号装置へ配送する（ステップ１１、１２）。暗号装置の動作は、実施の形態１、２と同様である。

【００１９】以上のように、ネットワーク管理者が指定した通信グループ内の通信が透過中継となる場合に、ネットワーク管理者へ問い合わせるため、セキュリティが低下することを確認でき、誤って通信グループを指定してしまった場合にも事前に検出できる。

【００２０】実施の形態４．実施の形態３では、ネットワーク管理者が指定する通信グループが他の通信グループと重複していないが、本実施の形態では、重複する場合の実施の形態を以下に示す。図１３は、ネットワーク管理者が指定した複数の通信グループが重複するような場合のネットワーク構成図である。次に図１４を用いて動作を説明する。ネットワーク管理者は、ネットワーク構成図を表示し（ステップ１）、ネットワーク構成図上のエリア、通信端末及び暗号装置を選択し、通信グループ１を指定し（ステップ２）、この通信グループのセキュリティレベル（図の例では＝１）を設定する。続いて、前記と同様の手順で通信グループ２、セキュリティレベル＝２を設定する（ステップ２、１６）。通信グループの指定が終了したら（ステップ１７）、前記実施の形態と同様にすべての通信経路を検索し、通信経路にある暗号装置に対して、同一セキュリティレベルの通信グループに属する暗号装置が存在するかチェックする（ステップ１８）。同じレベル暗号装置がない存在しない場合は、通信経路の両端のアドレスをこの暗号装置の暗号

通信制御テーブルの宛先、送信元アドレスに設定し、制御コードに廃棄を設定する（ステップ９）、存在する場合は、暗号通信制御テーブルに通信経路の両端のアドレス、制御コードに暗号を設定し（ステップ１３）、暗号鍵を生成して暗号通信制御テーブルに設定し（ステップ１４）、暗号装置へ配送する（ステップ１１、１２）。暗号装置の動作は、実施の形態１と同様である。

【００２１】以上のように、ネットワーク管理者が指定する通信グループにセキュリティレベルを設け、通信グループが重複する場合、セキュリティレベルを比較するので、暗号通信グループの設定が柔軟になり、また、通信グループが重複しても通信端末間通信のセキュリティを保つことができる。

【００２２】

【発明の効果】以上のように、第１の発明によれば、暗号ＶＰＮ管理装置に表示されたネットワーク構成図を使用して通信グループを指定し、通信端末の通信経路を求め、暗号通信制御テーブルを作成し、暗号装置に配送するようにしているので、通信端末間の通信における通信経路が明確化され、通信端末のアドレスを元に人手により暗号通信情報を設定するより操作ミスを少なくできる。通信端末からの通信データを受信した場合も、暗号装置は暗号通信テーブルを保持しているため、鍵探索バケットを送信する必要がないので暗号通信開始時のオーバヘッドをなくすことができ、また企業ネットワークの安全性を損なうことなく暗号通信を実現できる。

【００２３】第２の発明によれば、暗号ＶＰＮ管理装置から暗号通信制御テーブルと暗号鍵を合わせて配送するようにしているので、保持している鍵が異なっているため鍵ＩＤが合っているにもかかわらず通信できないといった通信の不通状態を防ぐことができる。

【００２４】第３の発明によれば、ネットワーク管理者は指定した通信グループ内の通信が透過中継となる場合に、問い合わせるため、ネットワーク管理者はセキュリティが低下することを確認でき、誤ってエリア、通信端末を指定してしまった際にも事前に検出できる。

【００２５】第４の発明によれば、ネットワーク管理者が指定する通信グループにセキュリティレベルを設け、通信グループが重複する場合、セキュリティレベルを比較するので、暗号通信グループの設定が柔軟になり、また、通信グループが重複しても通信端末間通信のセキュリティを保つことができる。

【図面の簡単な説明】

【図１】　実施の形態１、２におけるネットワーク構成図である。

【図２】　実施の形態１の暗号ＶＰＮ管理装置を示すブロック図である。

【図３】　この発明の暗号装置を示すブロック図である。

【図４】　実施の形態１の暗号装置１における暗号通信制御テーブルである。

【図５】　この発明の管理通信フレームである。

【図６】　実施の形態１における暗号ＶＰＮ管理装置の処理を示すフローチャートである。

【図７】　実施の形態２の暗号ＶＰＮ管理装置を示すブロック図である。

【図８】　実施の形態２の暗号装置１における暗号通信制御テーブルである。

【図９】　実施の形態２における暗号ＶＰＮ管理装置の処理を示すフローチャートである。

【図１０】　実施の形態３におけるネットワーク構成図である。

【図１１】　実施の形態３の暗号装置１における暗号通信制御テーブルである。

【図１２】　実施の形態３における暗号ＶＰＮ管理装置の処理を示すフローチャートである。

【図１３】　実施の形態４におけるネットワーク構成図である。

【図１４】　実施の形態４における暗号ＶＰＮ管理装置の処理を示すフローチャートである。

【図１５】　従来例における暗号通信の接続図である。

【図１６】　従来例におい暗号鍵テーブルである。

【図１７】　従来例における鍵探索バケットである。

【符号の説明】

１　暗号ＶＰＮ管理装置
２　送受信処理部
３　入力制御部
４　構成表示部
５　テーブル演算部
６　暗号処理部
７　テーブル配送部
１０、３３、３４、６０、６１、７１、７２、７３、７４、７５　暗号装置
１１　パブリックポート
１２、１９　送受信処理部
１３　暗号化、復号部
１４　透過中継部
１５　廃棄部
１６　暗号通信制御テーブル
１７　テーブル管理部
１８　テーブル復号部
１９　ローカルポート
３０、３２　ルータ
３１、３６、３７、３８、７６、７７、７８　通信端末
３９　暗号ＶＰＮ管理装置
５２　暗号鍵生成部
８１　ヘッダ
８２　送信元端末アドレス
８３　宛先端末アドレス

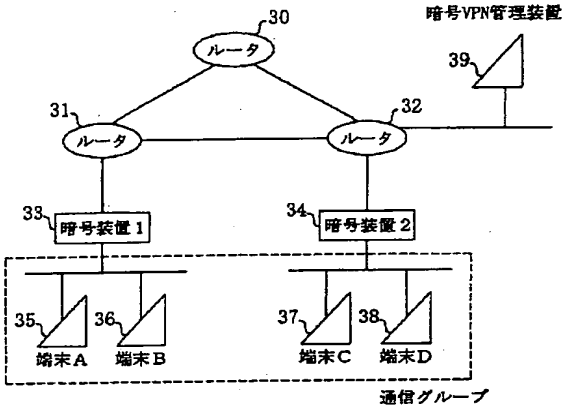
11

８４　ローカルポート暗号鍵情報
８５　パブリックポート暗号鍵情報

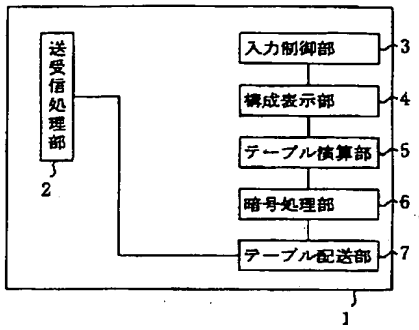
12

＊９１　ヘッダ
＊　９２　暗号通信制御テーブル

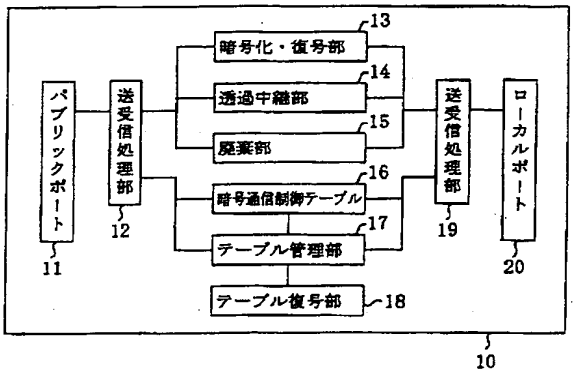
【図１】



【図２】



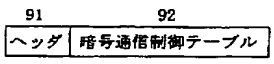
【図３】



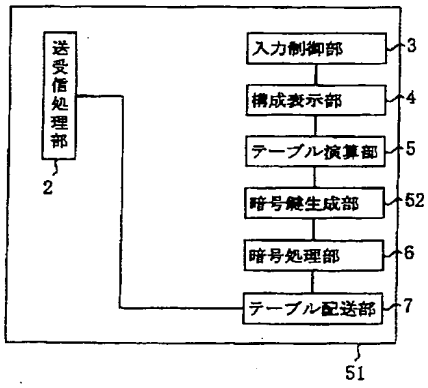
【図４】

宛先	送信元	制御コード	暗号鍵ＩＤ
C	A	暗号	1
D	B	暗号	1
C	B	暗号	1
D	A	暗号	1

【図５】



【図７】



【図８】

宛先	送信元	制御コード
C	A	暗号
D	B	暗号
C	B	暗号
D	A	暗号
暗号鍵		

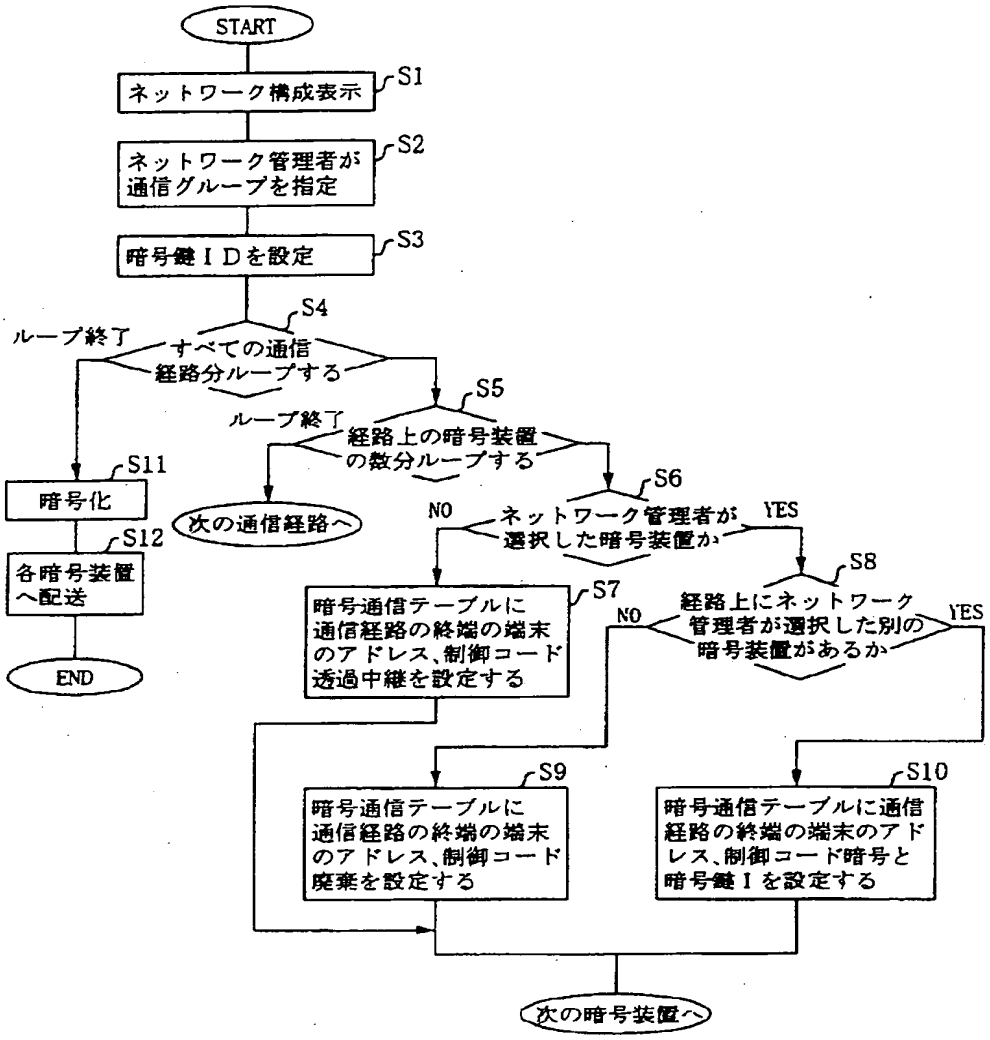
【図１１】

宛先	送信元	制御コード
C	A	透過中継
D	B	透過中継
C	B	透過中継
D	A	透過中継

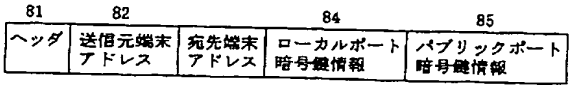
【図１６】

通信端末	処理方法	保持時間
A-B	ID 1	600
A-C	廃棄	600

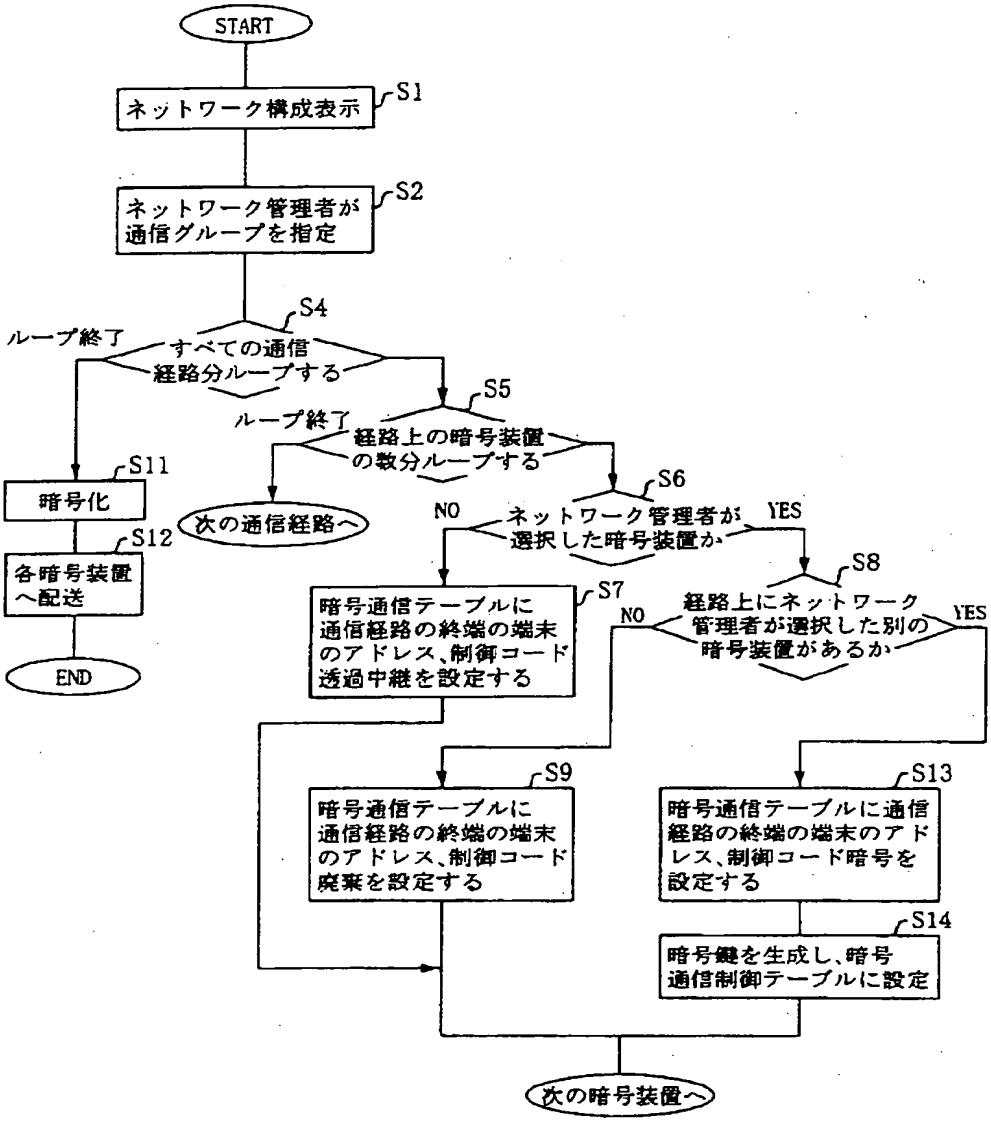
【図６】


START
ネットワーク構成表示
S1
ネットワーク管理者が通信グループを指定
S2
暗号鍵ＩＤを設定
S3
S4
すべての通信経路分ループする
ループ終了
S5
経路上の暗号装置の数分ループする
ループ終了
次の通信経路へ
S6
NO
ネットワーク管理者が選択した暗号装置か
YES
S8
経路上にネットワーク管理者が選択した別の暗号装置があるか
NO
YES
S7
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード透過中継を設定する
S9
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード廃棄を設定する
S10
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード暗号と暗号鍵Ｉを設定する
次の暗号装置へ
S11
暗号化
S12
各暗号装置へ配送
END

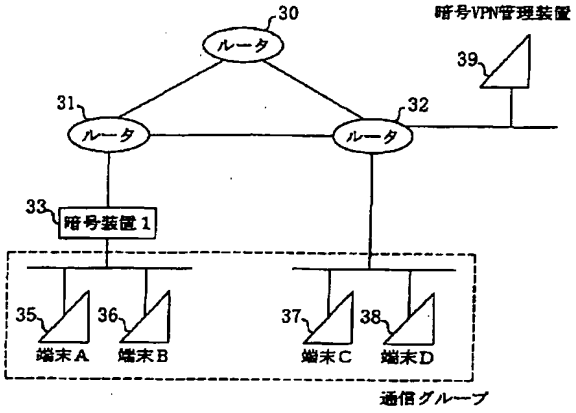
【図１７】


81
82
84
85
ヘッダ
送信元端末アドレス
宛先端末アドレス
ローカルポート暗号鍵情報
パブリックポート暗号鍵情報

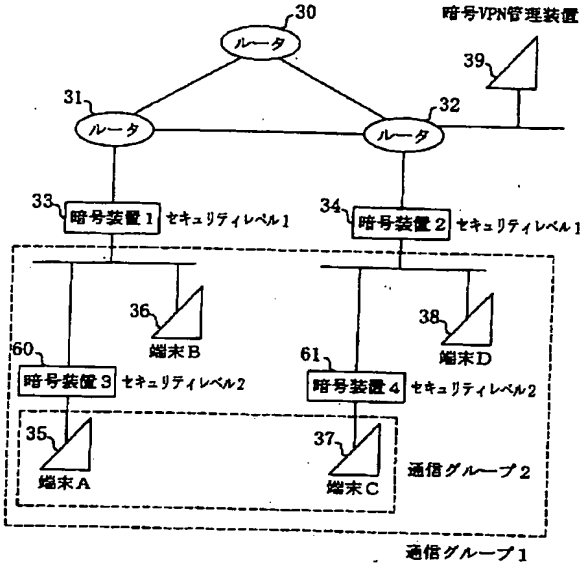
【図９】


START
ネットワーク構成表示
S1
ネットワーク管理者が通信グループを指定
S2
S4
すべての通信経路分ループする
ループ終了
S5
経路上の暗号装置の数分ループする
ループ終了
S11
暗号化
S12
各暗号装置へ配送
END
次の通信経路へ
S6
NO
ネットワーク管理者が選択した暗号装置か
YES
S8
S7
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード透過中継を設定する
NO
経路上にネットワーク管理者が選択した別の暗号装置があるか
YES
S9
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード廃棄を設定する
S13
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード暗号を設定する
S14
暗号鍵を生成し、暗号通信制御テーブルに設定
次の暗号装置へ

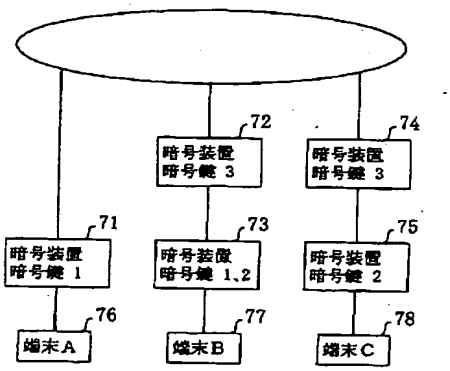
【図１０】


30
暗号VPN管理装置
ルータ
39
31
ルータ
32
ルータ
33
暗号装置１
35
端末A
36
端末B
37
端末C
38
端末D
通信グループ

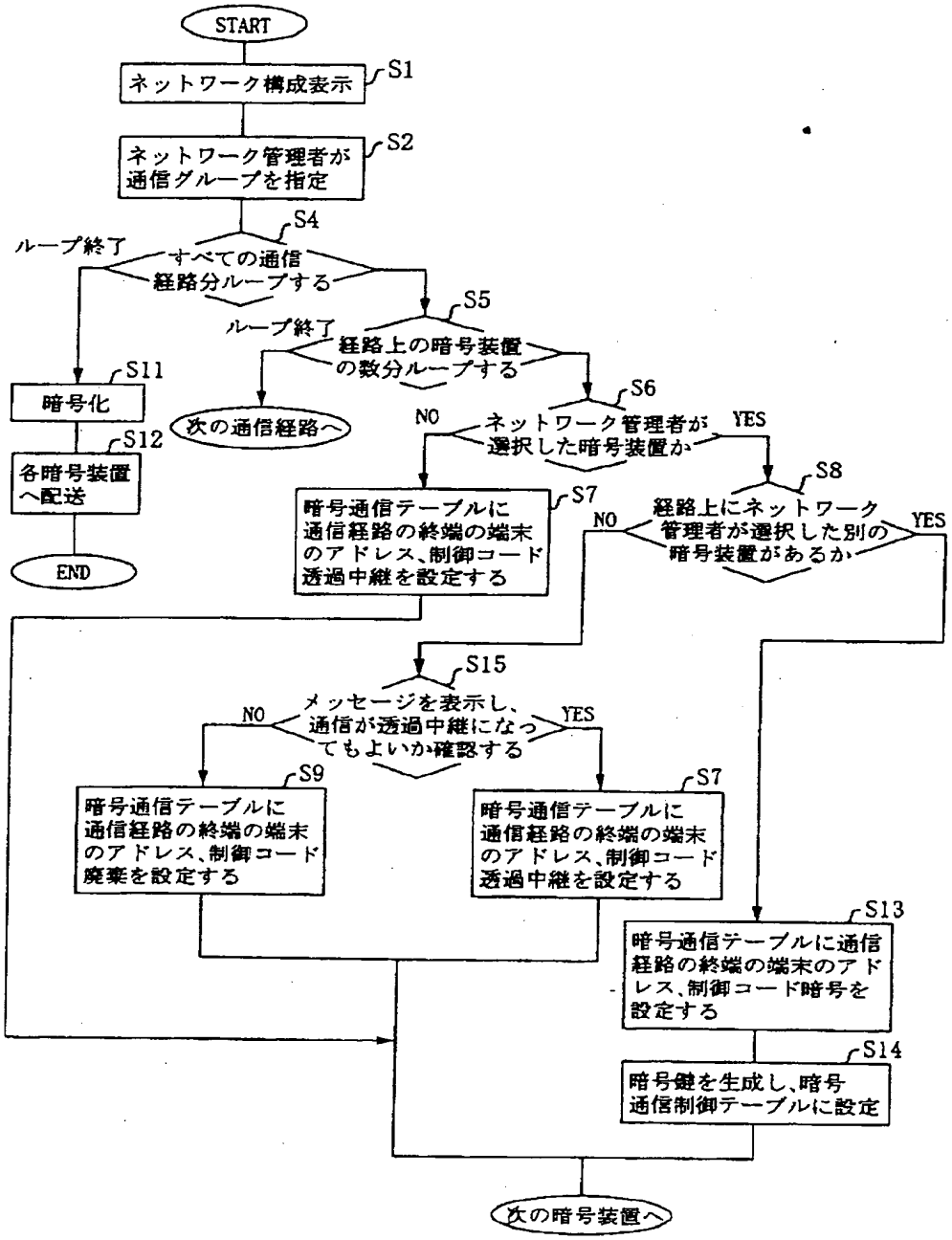
【図１３】


30
暗号VPN管理装置
ルータ
39
31
ルータ
32
ルータ
33
暗号装置１
セキュリティレベル１
34
暗号装置２
セキュリティレベル１
36
端末B
38
端末D
60
暗号装置３
セキュリティレベル２
61
暗号装置４
セキュリティレベル２
35
端末A
37
端末C
通信グループ２
通信グループ１

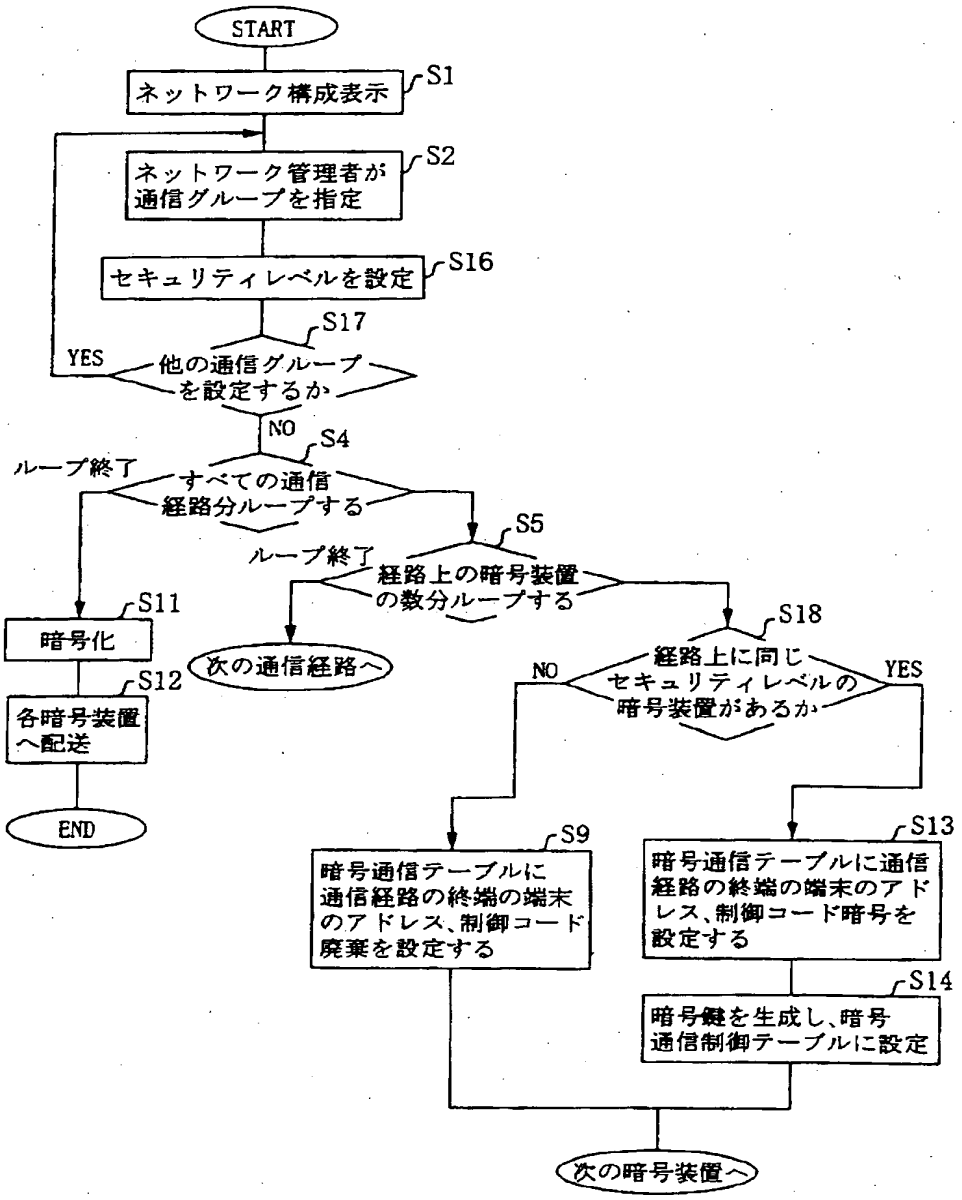
【図１５】


72
暗号装置
暗号鍵 3
74
暗号装置
暗号鍵 3
71
暗号装置
暗号鍵 1
73
暗号装置
暗号鍵 1、2
75
暗号装置
暗号鍵 2
76
端末A
77
端末B
78
端末C

【図１２】


START
ネットワーク構成表示
S1
ネットワーク管理者が通信グループを指定
S2
S4
すべての通信経路分ループする
ループ終了
S5
経路上の暗号装置の数分ループする
ループ終了
次の通信経路へ
S6
NO
ネットワーク管理者が選択した暗号装置か
YES
S8
経路上にネットワーク管理者が選択した別の暗号装置があるか
NO
YES
S7
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード透過中継を設定する
S11
暗号化
S12
各暗号装置へ配送
END
S15
NO
メッセージを表示し、通信が透過中継になってもよいか確認する
YES
S9
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード廃棄を設定する
S7
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード透過中継を設定する
S13
暗号通信テーブルに通信経路の終端の端末のアドレス、制御コード暗号を設定する
S14
暗号鍵を生成し、暗号通信制御テーブルに設定
次の暗号装置へ

【図１４】



フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
H04L 9/36		H04L 11/20	B
12/66			102D
12/56			

(72)発明者　渡邊　晃
東京都千代田区丸の内二丁目２番３号　三
菱電機株式会社内